mc garr SOLICITORS

12 City Gate, Lower Bridge St., Dublin 8 Ireland
Tel 01 635 1580 Fax 01 635 1578
eMail info@mcgarrsolicitors.ie Web www.mcgarrsolicitors.ie

Our Ref: BRA007/01/SMcG Your Ref: 2nd April 2019

The Data Protection Commission
21 Fitzwilliam Square South
Dublin 2
D02 RD28
Ireland

Re: Formal Complaint by Dr. Ryan regarding IAB Europe A.I.S.B.L website

Dear Commission,

1. We are instructed by Dr Johnny Ryan to make a formal complaint to the Data Protection Commission (DPC) regarding the "cookie wall", "cookie notice", and guidance regarding cookies of IAB Europe A.I.S.B.L. (BE 0812.047.277), having its registered offices at 1040 Brussels (Belgium), Rond-Point Schuman, 11 ("IAB Europe"), who have as their purpose the representation of the "behavioural advertising" industry ("the industry"). Dr Ryan has a personal and professional interest in this complaint:

   Dr Ryan is Chief Policy & Industry Relations Officer of Brave Software, a private web browsing company with offices in San Francisco and London. He is the author of two books on matters relating to the Internet, and its regulation. Dr Ryan is a member of the World Economic Forum's expert network. He was previously Chief Innovation Officer of The Irish Times, and a Senior Researcher at the Institute of International & European Affairs.

   He has sought to access the website of IAB Europe on multiple occasions (most recently on the 15th March 2019) and on each occasion, he has been presented with a 'cookie wall' (a requirement to agree to all cookies set by the domain controller, without which the information on the domain cannot be accessed or read). See the attached screen shots for an image of same.

   Our client's work and personal research requires him to access the information accessible on the IAB Europe website, but to do so he is required to provide an invalid form of consent to "cookies for functional and analytical purposes." The website confirmed that "Some cookies used by third party providers may be used for targeted advertising purposes."

2. The purpose of this complaint is to seek a formal decision by the Data Protection Commissioner, as the Data Protection Agency in the EU member state in which our client resides, that IAB Europe's use of a cookie wall (which has been implemented in line with IAB Europe's guidelines for industry on the use of cookie walls) is incompatible with the General Data Protection Regulation, the e-Privacy Directive and the Charter of Fundamental Rights, and that our client's personal data consequently been unlawfully processed.

Overview

3. The website www.iabeurope.eu is operated by IAB Europe AISBL, and is described in its general terms[1] as "a corporate website providing information and news about IAB Europe, its member network and the digital industry (e.g. press releases, research, policy news, events)."

4. This website prevents a visitor from viewing any web pages unless the visitor clicks "I agree" to a "cookie notice" that is displayed when the page first loads. This notice states:

> "IAB Europe uses cookies for functional and analytical purposes. Some cookies used by third party providers may be used for targeted advertising purposes.
>
> - Click on 'I Agree' to agree to the use of cookies of IAB Europe and third parties.
> - Click on 'More info' for more information about the processing of the (personal) data that can be collected and processed by IAB Europe and third parties.
> - For additional details, please read our privacy policy."

A person must click the "I accept" button at the bottom of this notice to gain access to the website.

5. There are three causes for concern.

[1] https://www.iabeurope.eu/general-terms-of-use/

i. Consent walls are prohibited by the GDPR[2]. Dr Ryan's personal data was unlawfully processed by IAB Europe as a result of the IAB Europe cookie wall on its website.

ii. IAB Europe has provided inadequate information about what is being consented to, what data will be processed for which purpose, and how data rights can be exercised. No consent based on the 'cookie notice' provided can meet the requirement for 'freely given, specific, informed and unambiguous indication of the data subject's wishes'[3]

iii. IAB Europe has put itself forward as the primary designer of the online advertising industry's data protection notices, and has widely promoted the notion that access to content can be made conditional on consent for data processing that is not necessary for the requested service to be delivered. This makes our client's complaint one of both a systemic, as well as personal, nature.

6. In the light of these ongoing breaches of the relevant regulations and statutes detailed below, the Data Protection Commissioner is requested to:

i. Issue a formal decision in response to our client's complaint.

ii. To invoke its powers under Article 58 of the GDPR to order IAB Europe to cease processing any personal data collected or obtained, and in all instances where IAB Europe relies on the complained-of cookie wall consent to give colour of law to such processing.

iii. If required, to seek mutual assistance under Article 60 et al of the GDPR from the DPA of IAB Europe's jurisdiction of establishment, Belgium.

iv. Open a systemic investigation of the compatibility of IAB Europe's guidance on the issue of cookie walls with EU Data Protection laws.

Grounds of Complaint

i. IAB Europe's website's cookie wall

7. Article 4(11) of the GDPR sets out the requirements for valid consent.

> "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to

[2] See Section C below.
[3] Article 4(11) General Data Protection Regulation

the processing of personal data relating to him or her;"

8. Article 5 (1) a of the GDPR requires that data be "processed lawfully, fairly, and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')".

9. Article 7 (4) of the GDPR reflects the requirements in assessing whether consent has been freely given:

> "When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

10. Recital 42 of the GDPR observes that users should be able to "refuse or withdraw consent without detriment". Recital 43 states:

> "...Consent is presumed not to be freely given if ... the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance."

Our client is aware that this is a matter which has been addressed by the Dutch DPA at https://autoriteitpersoonsgegevens.nl/nl/nieuws/websites-moeten-toegankelijk-blijven-bij-weigeren-tracking-cookies and by the Bavarian State Office for Data Protection Supervison (BAYLDA) in their Safer Internet day inspection of consents[4].

Our client's data has been collected, shared and otherwise processed without valid consent being obtained, but in circumstances where consent is the only legal basis provided for and/or cited by the Data Controller or Controllers. The consequence is that our client's personal data has been processed, and continues to be shared and processed without a lawful basis.

ii. Inadequate information:

11. Upon clicking the button titled "more info" a notice is displayed. A copy of this notice is attached for ease of reference. There are several problems with the information in this

[4] https://www.lda.bayern.de/media/sid_ergebnis_2019.pdf

"more info" notice, together with the initial cookie notice.

i. Upon clicking "more info" is becomes apparent that the cookie wall message is actually a catch-all request for consent to use local storage, perhaps conceived as a nod to the ePrivacy Directive, rather than a request to process personal data.

ii. The "more info" notice conflates multiple processing purposes that must all be accepted together by clicking "accept" before a visitor can enter the website. These include YouTube[i], MailChimp data base and communications, Google analytics, social media widgets, the processing of purchase orders, personalisation of the website, and website improvement, and DoubleClick's profiling for ad targeting etc. via YouTube).

In addition, the "privacy policy" lists 27 processing purposes, including some purposes like human resources that are internal to the organisation. It is not possible to know whether clicking "accept" on IAB Europe's cookie wall is intended to signal acceptance of the "more info" purposes or the "privacy policy" purposes, or both.

In any case, the lack of granularity in IAB Europe's single "accept" everything button is contrary to the purpose limitation principle in Article 5 (1) b of the GDPR, which requires that consent be requested in a granular manner for "specified, explicit" data processing purposes. There must be granular consent for each specific processing purpose for which consent is the legal basis. Recital 32 of the GDPR observes that:

> "Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them."

Recital 42 of the GDPR observes that:

> "Consent is presumed not to be freely given even if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case"

In the Working Party guidelines on consent, European Data Protection Authorities observed that:

> "data subjects should be free to choose which purpose they accept, rather than having to consent to a bundle of processing purposes. ... If the controller has conflated several purposes for processing and has not

attempted to seek separate consent for each purpose, there is a lack of freedom. This granularity is closely related to the need of consent to be specific .... When data processing is done in pursuit of several purposes, the solution to comply with the conditions for valid consent lies in granularity, i.e. the separation of these purposes and obtaining consent for each purpose."[5]

iii. Furthermore, IAB Europe's "more info" information about data processing purposes is inadequate. The "more info" notice mentions broad uses of data by third parties: Google "collecting information to personalize advertising", and Facebook, Linkedin, and Twitter "sharing our content on social media channels".

In its 2013 opinion on "purpose limitation", the Article 29 Working Party set the scope of what an individual purpose is. A purpose must be "sufficiently defined to enable the implementation of any necessary data protection safeguards," and must be "sufficiently unambiguous and clearly expressed."[6]

The test is "If a purpose is sufficiently specific and clear, individuals will know what to expect: the way data are processed will be predictable."[7] The objective is to prevent "unanticipated use of personal data by the controller or by third parties and in loss of data subject control".[8]

A lawful purpose must be specific, transparent and predictable.[9] It must be describable to the extent that the processing undertaken for it would not surprise the person who gave consent for it. This does is not the case with IAB Europe's website. Our client cannot know what Facebook, Google, etc. will do with his personal data once it is passed via the IAB Europe website, or how long they will do it for, or whether they will pass it on to other parties. Independently obtained information, such as that outlined at Footnote 3 above regarding YouTube and Google, indicates that there is scope for very significant additional processing, and the sharing of data with numerous actors.

iv. The "more info" notice does not make clear who the controller is for the various purposes. The notice does appear to acknowledge that IAB Europe's decision to install YouTube, and various social media tools on its websites means that visitors' personal data will be processed by Google, Facebook, LinkedIn, Twitter, etc. But IAB Europe does not appear to recognise that it is a controller of this processing by the companies it has chosen to install on its website. This is despite the fact that it is a

[5] "Guidelines on consent under Regulation 2016/679", Article 29 Working Party, 28 November 2017, p. 11.
[6] "Opinion 03/2013 on purpose limitation", Article 29 Working Party, 2 April 2013, p. 12.
[7] "Opinion 03/2013 on purpose limitation", Article 29 Working Party, 2 April 2013, p. 13.
[8] "Guidelines on consent under Regulation 2016/679", Article 29 Working Party, 28 November 2017, p. 12.
[9] "Opinion 03/2013 on purpose limitation", Article 29 Working Party, 2 April 2013, p. 13.

requirement of the YouTube Terms of Use, for example, that

> "You must use commercially reasonable efforts to disclose clearly, and obtain consent to, any data collection, sharing and usage that takes place on any site, app, email publication or other property as a consequence of your use of Google products"

v. The "more info" notice does not explain the right to withdraw consent at any time from IAB Europe and the other companies that it appears that IAB Europe has passed personal data to. Nor does it explain how to exercise this right. Article 7 (3) of the GDPR requires that a person be told that they can withdraw consent at any time, and that consent shall be as easy to withdraw as it was to give.

12. The information in IAB Europe's longer "privacy policy" document (a copy of which is attached for ease of reference) is also inadequate, and it appears to be difficult to request data, and impossible to withdraw consent.

i. Lack of clear legal basis for processing.
IAB Europe does not provide information about what data are collected for what purpose, and what legal basis is relied on for that purpose. IAB Europe's policy notice says "we may rely on one or more of the following legal bases, depending on the circumstances".[10] It is therefore not possible for a visitor to the website to know what legal basis is used for what purpose. Nor does IAB Europe provide information about which data are collected for what specific purpose.

To take only one example, to show the insufficiency of this statement to meet the requirements of informed consent, the Google Privacy Policy[11] specifically covers YouTube: and outlines very considerable secondary data processing that will be applied to the data of anyone loading a page containing an embedded YouTube video.

In addition, the YouTube API Services Terms of Service (EMEA) (which applies, amongst other things, to embedding videos in websites or apps) seeks to bind the Data Controller of a website to be responsible for their worker or agent's use of the software.

> "If you are using the YouTube API Services on behalf of someone else (such as your employer), you warrant that you have authority to bind that person or entity to the Agreement and by accepting the Agreement, you are doing so on behalf of that person or entity (and all references to "you"

[10] IAB Europe privacy policy, section 4.
[11] Google Privacy Policy, https://www.google.com/policies/privacy/

in the Agreement refers to that person or entity)."[12]

It then goes on to pass responsibility for obtaining consents for the data being passed to YouTube onto that Data Controller body.

> "Without limiting Section 5 (Compliance with Laws), you will comply with all applicable privacy laws and regulations, including those applying to Personal Data. Each API Client will provide and adhere to a published privacy policy that clearly and accurately describes to its users what user information you and your API Client access, collect and store , and how and why you and your API Client use, process, and share such information (including for advertising) with us and other third parties." "

(An API client in this case means "a website or software application (including a mobile application) developed by you that accesses, or uses, the YouTube API Services." This includes IAB Europe's site with YouTube video embeds.)

And Section 9.2 specifically recognises the data protection burden of embedding a YouTube video, and addresses it by simply putting that burden on the Data Controller to comply

"For users in the European Union, you and your API Client(s) must comply with the EU User Consent Policy currently located at http://www.google.com/about/company/user-consent-policy.html."

The Google EU specific user policy, which covers YouTube, states:

"When using Google products that incorporate this policy, certain disclosures must be given to and consents obtained from end users in the European Union where EU data protection law requires such disclosures and consents.
For end users in the European Union:
You must use commercially reasonable efforts to disclose clearly, and **obtain consent to, any data collection, sharing and usage** that takes place on any site, app, email publication or other property as a consequence of your use of Google products;" "

Google/YouTube know that the embedding of a video triggers onerous and difficult requirements to obtain consent for an extremely wide-ranging set of subsequent uses which they put the data to- including associating that information with the rest of the

[12] Section 3.3, **YouTube API Services Terms of Service (EMEA), https://developers.google.com/youtube/terms/api-services-terms-of-service-emea**
[13] https://developers.google.com/youtube/terms/api-services-terms-of-service-emea
[14] https://www.google.com/about/company/user-consent-policy.html

information they may hold on that data subject from other sources, including gmail, advertising on other sites etc.

They have simply created a series of Data Processor agreement documents which, taken together, seek to push that heavy burden (and compliance risk) onto the Data Controller.

There is a more privacy-friendly method of serving YouTube videos offered by the site. Trackers which would otherwise be dropped when the page loaded with an embedded video are instead only triggered when the data subject presses play on the video.

This system can be forced on a site by using only the Privacy Enhanced embed option-

While normal embed code loads from youtube.com:
<iframe width="560" height="315"
src="https://www.youtube.com/embed/zjVqHVo0nq0" frameborder="0"
allow="autoplay; encrypted-media" allowfullscreen></iframe>

The privacy enhanced version will load from youtube-nocookie.com
<iframe width="560" height="315" src="https://www.youtube-nocookie.com/embed/zjVqHVo0nq0" frameborder="0" allow="autoplay; encrypted-media" allowfullscreen></iframe>

None of this information is given to our client, or any other data subject, prior to their processing their data. In addition, it is clear that there are other, less onerous processing options available to the Data Controller(s) but that they have not chosen to engage with them.

ii. Inadequate information regarding retention of data periods.

IAB Europe does not provide adequate information about duration of storage. IAB Europe's criteria for determining the duration of storage include the following:

> "Where your personal data is necessary in connection with the lawful purposes set out in this Privacy Policy, for which we have a valid legal basis".

Since the "privacy policy" lists twenty seven purposes, the visitor has no way to know what duration of storage actually applies.

iii. Lack of information about what third parties do with data.

IAB Europe claims that the social media widgets that it has chosen to install on its website "may collect your IP address, which page you are visiting on our Websites, and may set a cookie to enable the Feature to function properly".[15] It is not clear

[15] IAB Europe privacy notice, section 14.3

what is being done with the visitor's data by what party. For example, there is no information about what these features are, what they do with whatever data they process, or why they do so.

IAB Europe does not accept it is the controller of the processing undertaken by social media widgets that it has chosen to install on its website. It says that

> "Your interactions with these Features are governed by the privacy policy of the company providing it."[16]

iv. Problems with how data rights can be exercised.

IAB Europe claims that the withdrawal of consent "does not prevent any processing of personal data on any other available legal bases".[17] This is an inappropriate clause in circumstances where, as with our client's data, the only legal basis which has been advanced has been consent.

IAB Europe's failure to specify what legal basis it relies on for what purpose means that our client cannot know what rights he can exercise. For example, one cannot object to processing which is held out as being on the basis of consent if the data controller asserts there are other, undisclosed bases.

Although IAB Europe is happy to respond to e-mail requests for testimonials on its site to be deleted,[19] it insists that data deletion requests be made in writing, and only by means of post.[20] It specifies that this request must be accompanied by certain materials, but does not articulate what these materials are. This appears to render it impossible or difficult to exercise the rights to access, rectification, or erasure.

Section 12:

> "The User or the Member may also request access, ask for rectification and for deletion of their personal data, except those which IAB Europe are legally obliged to retain, from IAB Europe's database by addressing a written request, accompanied with, to the data controller at the following address: IAB Europe, rue Bara, 175, B-1070 Brussels."

[16] IAB Europe privacy notice, section 14.3
[17] IAB Europe privacy notice, section 12.
[19] IAB Europe privacy notice, section 14.1
[20] IAB Europe privacy notice, section 12.

13. IAB Europe's lack of information is particularly troubling to our client because this organisation has taken it upon itself to advise the online advertising technology industry on how to comply with data protection law. The IAB Europe website includes "GDPR implementation guidelines", for example, and recommends that media organisations and advertising technology and tracking companies adopt its GDPR consent mechanism. The cookie wall on its website is a concrete example of the operation of its guidelines on consent. The continued promotion of these guidelines therefore raises systemic data protection concerns with EU-wide implications.

iii. IAB Europe's guidelines on consent

14. IAB Europe describes its mission as including "help[ing] member companies and the digital advertising industry interpret and comply with EU rules on data protection and privacy".[21] In November 2017 IAB Europe published a paper on consent that it offers as industry guidance (**"guidance"**).[22] IAB Europe continues to promote this paper.

15. In the guidance, IAB Europe claims that "Private companies are allowed to make access to their services conditional upon the consent of data subjects":[23]

> "The GDPR does not establish a prohibition on making access to a service conditional on consent. The ePrivacy Directive clarifies that access to "website content may still be made conditional on the well-informed acceptance of cookies" and use of similar tracking technologies. Digital services, such as websites or apps are generally permitted to require users to consent to the collection their personal data through cookies or similar technologies before allowing them to use a service."[24]

The effect of this passage is to tell major media organizations, tracking companies, and advertising technology companies that they can sidestep the GDPR, and rely instead on the ePrivacy Directive which, IAB Europe claims, is more lax.

16. IAB Europe presents the following argument to justify this:

[21] "GDPR implementation", IAB Europe (URL: https://www.iabeurope.eu/category/policy/gdpr-implementation/)
[22] "Consent, Working Paper 03/2017", IAB Europe, 28 November 2017.
[23] "Consent, Working Paper 03/2017", IAB Europe, 28 November 2017, p. 4.
[24] "Consent, Working Paper 03/2017", IAB Europe, 28 November 2017, p. 9.

> "Article 95 GDPR on the relationship of the GDPR with the ePrivacy Directive establishes that the ePrivacy Directive's more specific rules prevail over rules of the GDPR."25

This is, of course, a misreading of the relationship between the two statutes.

17. Article 95 of the GDPR states:

> "This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC."[26]

Article 95 is triggered only if there is a specific obligation with the same objective set out in the ePrivacy Directive. For example, as the EDPB recently observed in its opinion on the interplay between the ePrivacy Directive and the GDPR:

> "They [GDPR and ePrivacy Directive] both provide for an obligation to ensure security, as well as an obligation to notify personal data breaches to the competent national authority and the data protection authority, respectively. These obligations are applicable in parallel under the two different pieces of legislation, according to their respective scopes of application. Clearly, an obligation to notify under both acts, once in compliance with the GDPR and once in compliance with national ePrivacy legislation would constitute an added burden without immediate apparent benefits for data protection."[27]

[25] "Consent, Working Paper 03/2017", IAB Europe, 28 November 2017, p. 7.
[26] Article 95, General Data Protection Regulation.
[27] "Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities", European Data Protection Board, 12 March 2019, p.15.

18. IAB Europe claims that Recital 25 of the ePrivacy Directive triggers Article 95. However, Recital 25 is not an Article of the GDPR, and has no direct legal effect. Even if this were not the case, the relevant phrase in Recital 25 that IAB Europe has selected, "website content may still be made conditional on the well-informed acceptance of cookies", does not impose an obligation. In fact, it provides a narrow allowance, which is quite the opposite.

19. There is a further problem in IAB Europe's guidance to the digital media industry on this particular point. Article 95 of the GDPR applies only to "electronic communications services". These are defined in Directive 2002/21/EC as:

> "Electronic communications service means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks".[28]

This definition makes it clear that media "providing, or exercising editorial control over, content" are explicitly excluded in the definition of electronic communications services. This means that Article 95 does not apply to IAB Europe's website, or to other websites with editorial control over content.

20. Aside from the fact that Article 95 is not triggered, there are additional concerns about IAB Europe's guidance for Europe's online media companies regarding Recital 25 of the ePrivacy Directive. IAB Europe's guidance cites only a fragment of one of the Recital's sentences to claim that tracking walls are permissible for all websites:

> "website content may still be made conditional on the well-informed acceptance of cookies".[29]

[28] Article 2, paragraph c, of Directive 2002/21/EC of The European Parliament and of The Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

[29] "Consent, Working Paper 03/2017", IAB Europe, 28 November 2017, p. 9.

The complete sentence from Recital 25 of the ePrivacy Directive is (with missing parts in bold):

> "**Access to specific** website content may still be made conditional on the well-informed acceptance of a cookie **or similar device, if it is used for a legitimate purpose.**"[30]

The words "specific website content" and "legitimate purpose" that are excluded in IAB Europe's guidance are significant.

21. European data protection authorities observed in 2013 that the words "specific website content" meant that:

> "websites should not make conditional 'general access' to the site on acceptance of all cookies but can only limit certain content if the user does not consent to cookies".[31]

This, however, is exactly what IAB Europe has done with our client's personal data, and what it promotes as valid practise among its members in the media, tracking, and advertising industries.

22. Recital 25 of the ePrivacy Directive includes an example of what a legitimate purpose is: "such as to facilitate the provision of information society services...". Information society services are defined in Directive 98/34/EC as:

> "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of this definition: ... "at the individual request of a recipient of services" means that the service is provided through the transmission of data on individual request."32

[30] Recital 25, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[31] Working Document 02/2013 providing guidance on obtaining consent for cookies, Article 29 Working Party, p. 5.

[32] Article 1, paragraph 2 of Directive 98/48/EC of The European Parliament and of The Council of 20 July 1998 amending directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations.

23. Advertising profiling by Google (via the DoubleClick cookie dropped by the YouTube player installed on the IAB Europe website), and any other companies that IAB Europe has passed our client's personal data to, is not the service that the user visiting this website has requested.

24. IAB Europe has in the past claimed in a public statement that the definition of what an information society service is allows any and all tracking as part of accessing a site, if it is bundled together with accessing that site;

> "When a browser connects to a website it's making technically a request on the things that are being loaded. So it is technically requesting the content that is loaded on the site."[33]

However, a web browser is merely a piece of software. Loading a webpage which includes various forms of tracking cookies etc, the effect and content of which are not known or explained to the data subject loading that page, cannot be taken to be a 'request' for that tracking as, amongst other things, the person accessing the site does not know what tracking that site has enabled.

When its user tells it to visit the IAB Europe website, the web browser simply downloads whatever the website instructs it to. Claiming otherwise raises serious concerns about whether IAB Europe understands or accepts its data protection obligations.

Jurisdiction

Our client is resident in Ireland and makes his complaint to the Data Protection Commission, under the provisions of Article 57(f).

Exhaustion

On 20 September 2017, Dr Ryan raised these issues regarding IAB Europe's industry guidance with IAB Europe, through its branch in the UK, in an e-mail (a copy of which is attached for your reference), but received no substantive response.

[33] IAB Europe spokesperson quoted in "Cookie walls don't comply with GDPR, says Dutch DPA", TechCrunch, 8 March 2019 (URL: https://techcrunch.com/2019/03/08/cookie-walls-dont-comply-with-gdpr-says-dutch-dpa/).

On 30 November 2017, Dr Ryan published an analysis of the errors in IAB Europe's guidance.[34] Despite various online exchanges with representatives of IAB Europe since this date, there has not been a satisfactory outcome or meaningful response.

IAB Europe continues to use a cookie consent wall if data subjects want to access their website's contents, despite highly public and critical coverage of its position. This undermines the broader confidence in data protection among the online media and advertising industry with which the IAB is involved.

More specifically, our client is obliged to access the information made public on the IAB Europe website for both his personal research and his work. As a result his data continues to be processed in ways which fall outside any lawful grounds to do so.

We look forward to receiving your confirmation of our client's complaint and will be happy to address any additional queries you may have, or to provide any clarification you may require.

Yours faithfully

McGarr Solicitors

[34] Johnny Ryan, "Can websites use tracking walls to force consent under the GDPR", PageFair, 30 November 2017 (URL: https://pagefair.com/blog/2017/tracking-walls/).